Risk-Centered Practices

Julia H. Allen, Software Engineering Institute [vita[1]]

2006-10-30

This article establishes the role that risk management and risk assessment play in determining what security practices to implement and in what order. Risk management is critical in sustaining an acceptable level of security, given that it is not possible to be 100% secure.

Introduction

Why Are Risk-Centered Practices Necessary?

Given that it is impractical (and probably impossible) to ensure that an operational system is 100% secure at any point in time, security practitioners have found it useful to adopt risk management and assessment strategies to determine which security practices to deploy.

Risk assessment results are identified as a key prerequisite for sustainable operational security in Plan, Do, Check, Act[2], Table 1[3]. This topic is described in more detail in the BSI Risk Management[4] and Architectural Risk Analysis[5] content areas and applied to deployment and operations here.

Definition of Risk

Alberts [Alberts 05[6]] defines risk as “the possibility of suffering harm or loss.” Jones [Jones 05[7]] defines risk as “the probable frequency and probable magnitude of future loss.” NIST’s Special Publication *Risk Management Guide for Information Technology Systems* states the following [Stoneburner 02[8]]:

> Risk is the net negative impact of the exercise of a vulnerability, considering both the probability and the impact of occurrence. Risk management is the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level.
>
> Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations’ missions.

Questions to Ask

1. daisy:215 (Allen, Julia H.)
2. daisy:574 (Plan, Do, Check, Act)
3. daisy:574#tbl1 (Plan, Do, Check, Act)
4. daisy:68 (Risk Management)
5. daisy:194 (Architectural Risk Analysis)
6. daisy:583#Alberts05 (Deployment & Operations References)
7. daisy:583#Jones05 (Deployment & Operations References)
8. daisy:583#Stone02 (Deployment & Operations References)

In determining what risk-centered practices need to be deployed to ensure a more sustainable level of security, practitioners (and their managers) need to ask and answer the following questions [Allen 05[9]; BSI Governance & Management[10] article "How Much Security Is Enough?[11]"]:

- What is the value we need to protect?
- To sustain this value, what software, system, and information assets need to be protected? Why do they need to be protected? What happens if they’re not protected?
- What potential adverse conditions and consequences need to be prevented and managed? At what cost? How much disruption can we stand before we take action?
- How do we determine and effectively manage residual risk (the risk remaining after mitigation actions are taken)?
- How do we integrate our answers to these questions into an effective, implementable, enforceable security strategy and plan?

Principles that Argue for a Risk-Centered Approach

NIST Special Publication 800-27, *Engineering Principles for Information Technology Security* [Stoneburner 04[12]] identifies 33 principles for IT security, 7 of which are essential for deploying and operating a system using risk-centered practices. The 800-27 principle numbers are retained here to ease traceability to the publication:

- "Principle 5: **Reduce risk to an acceptable level.** The goal is to enhance mission/business capabilities by mitigating mission/business risk to an acceptable level. (See also BSI Governance & Management[13] article "How Much Security Is Enough?[14]" for a discussion of risk tolerance).
- Principle 6: **Assume that external systems are insecure.** Those responsible for deployment and operations should presume the security measures of an external system are different from those of a trusted internal system and deploy security practices accordingly.
- Principle 7: **Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.** A cost-benefit analysis should be conducted for each proposed security control. In some cases, the benefits of a more secure system may not justify the costs. In modifying or adjusting security goals, an acceptance of greater risk and cost may be inevitable.
- Principle 8: **Implement tailored system security measures to meet organizational security goals.** Implement lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only for the most critical assets.
- Principle 9: **Protect information while being processed, in transit, and in storage.** Select security measures that protect the confidentiality, integrity, and availability of information in all of these states.
- Principle 10: **Consider custom products to achieve adequate security.** In some instances, commercially available products may not be sufficient.
- Principle 11: **Protect against all likely classes of “attacks.”** Examples include passive monitoring, active network attacks, insider threat, attacks requiring physical access, social engineering, and the insertion of malicious code during software development and distribution."

[9] daisy:583#Allen05 (Deployment & Operations References)

[10] daisy:549 (Governance & Management)

[11] daisy:566 (How Much Security Is Enough?)

[12] daisy:583#Stone04 (Deployment & Operations References)

[13] daisy:549 (Governance & Management)

[14] daisy:566 (How Much Security Is Enough?)

Identifying the organization’s most critical assets and where those assets are most at risk should inform the selection and prioritization of security practices for deployment and operations.

Risk-centered practices that aid in security practice selection for deployment and operations include the following. These are listed in the order recommended for implementation.

1. Define the scope of the risk assessment. Ensure a clear and direct tie to business and mission objectives.
2. Identify information assets that are important to the organization. Focus risk assessment on those assets judged to be the most critical.
3. Identify asset owners and custodians.
4. Determine the criteria for accepting risks and the acceptable levels of risk, often referred to as risk tolerances or risk thresholds.
5. Identify the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats.
6. Assess the likelihood of threats and vulnerabilities.
7. Identify the impacts due to losses resulting from realized risks.
8. Identify risks and evaluate options for treatment of risks (accept, mitigate, avoid, transfer, share with a third party (such as a supplier)).
9. Identify practice-based protection strategies (control objectives and controls) that reduce risks to critical assets to levels that are within acceptable tolerances. Controls can be deployed to reduce likelihood and impact.

10Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.

11Identify approaches for managing residual risks that remain after protection strategies are adopted.

12Measure, review, and revise risk-centered practices. Re-assess risks periodically.

Table 1[15] (included at the end of this article) provides additional details and sources that expand these practices.

Description of Sources

The following sources were used to identify the risk-centered practices described above and expanded in Table 1.

BS 7799-3

British Standard 7799-3 *Guidelines for information security risk management* [BSI 06[16]] defines in detail the risk management practices identified in ISO 17799 [ISO 05a[17]] and ISO 27001 [ISO 05b[18]]. It states the following in its introduction:

> A process approach (for assessing risks, treating risks, and ongoing risk monitoring, risk reviews, and re-assessments) emphasizes the importance of (a) understanding business information security requirements and the need to establish policy and objectives for information security; (b)

[15] #tbl1

[16] daisy:583#BSI06 (Deployment & Operations References)

[17] daisy:583#ISO05a (Deployment & Operations References)

[18] daisy:583#ISO05b (Deployment & Operations References)

selecting, implementing, and operating controls in the context of managing an organization’s overall business risks; (c) monitoring and reviewing the performance and effectiveness of the Information Security Management System (ISMS) [19] to manage business risks; (d) continual improvement based on objective risk measurement.

BS 7799-3 includes useful information identifying categories of information security and organizational risk in Annex B and examples of assets, threats, vulnerabilities, and risk assessment methods in Annex A.

FIPS 199

With respect to identifying and categorizing information-related assets, NIST’s Special Publication *Standards for Security Categorization of Federal Information and Information Systems* provides useful guidance to establish

security categories for both information and information systems. The security categories are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals. Security categories are to be used in conjunction with vulnerability and threat information in assessing the risk to an organization [NIST 03[21]].

ISO/IEC 13335-3

This standard [BSI 98[22]] describes four options for risk analysis, from the deployment of baseline safeguards (referred to as minimum essential in Plan, Do, Check, Act[23], Table 2[24]) to a more comprehensive, detailed analysis recommended in Table 1 as follows:

- use the same baseline approach for all IT systems, regardless of risks facing the systems, and accept that the level of security may not always be appropriate
- use an informal approach, concentrating on IT systems that are perceived as facing exposure to high risks
- conduct detailed risk analysis using a formal approach for all IT systems
- conduct an initial "high level" risk analysis to identify IT systems exposed to significant risks and systems that are critical to the business. Perform a detailed risk analysis for these systems, and apply baseline security safeguards to all others.

ISO 13335-3 Annex B presents several approaches to establishing the value of information assets. Annex C lists a range of possible threat types. Annex D includes examples of common vulnerabilities.[25] Annex E presents a range of methods for risk analysis with four examples of how to use these methods.

[20] daisy:583#ISO05b (Deployment & Operations References)

[19] Defined in [ISO 05b[20]].

[21] daisy:583#NIST03 (Deployment & Operations References)

[22] daisy:583#BSI98 (Deployment & Operations References)

[23] daisy:574 (Plan, Do, Check, Act)

[24] daisy:574#tbl2 (Plan, Do, Check, Act)

[26] http://cve.mitre.org/

[25] The Common Vulnerabilities and Exposures web site[26] presents an up-to-date list of standardized names for vulnerabilities and other information security exposures.

OCTAVE

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation℠) is a method for managing information security risks. Unlike technology-focused assessments (such as vulnerability assessments or penetration tests), "OCTAVE is targeted at organizational risk and focused on strategic, practice-related issues. The intent of OCTAVE is to strike a balance between operational risk, security practices, and technology" [Alberts 03[27]].

The **three phases** of OCTAVE are

- Phase 1: Build Asset-Based Threat Profiles
  - Process 1: Identify senior management knowledge.
  - Process 2: Identify operational area knowledge.
  - Process 3: Identify staff knowledge.
  - Process 4: Create threat profiles.
- Phase 2: Identify Infrastructure Vulnerabilities
  - Process 5: Identify key components.
  - Process 6: Evaluate selected components.
- Phase 3: Develop Security Strategy and Plans
  - Process 7: Conduct risk analysis.
  - Process 8: Develop protection strategy.

Software Security: Building Security In

Chapter 2 of the book *Software Security: Building Security In* describes a **risk management framework** (RMF) comprising five stages [McGraw 06[28]]:

1. Understand the business context.
2. Identify the business and technical risks.
3. Synthesize and rank the risks.
4. Define the risk mitigation strategy.
5. Carry out fixes and validate.

This chapter also presents a comprehensive example of applying RMF to a server application with stringent first-to-market delivery date requirements, high availability requirements (99.999% uptime), and 100% transaction accuracy requirements to meet federal regulations.

Implementation Considerations

Risk-centered practices represent the state of practice for some organizations and systems. Field work in using the OCTAVE method[29] has shown that if a risk assessment is performed at a mid-level in the

[27] daisy:583#Alberts03 (Deployment & Operations References)

[28] daisy:583#McGraw06 (Deployment & Operations References)

[30] http://www.cert.org/octave/forum/agenda.html

[29] Some OCTAVE experience reports[30] are available on the CERT Web site.

organization, localized decisions can be made and acted on. Occasionally there are barriers to extrapolating these decisions to an organizational or system-wide level, which is often required to sustain successful improvement at the local level. An example is the need for a policy on incident reporting that enables local action but needs to be authored and sponsored at a broader organizational level to be enforceable.

If the organization performing system deployment and operations has no framework in which to accept localized risk assessment findings and deploy risk mitigation strategies to benefit the entire organization (and system), sustained improvement may be problematic. That said, an effective way to get started with risk-centered practices is described in the GAO's report *Information Security Risk Assessment: Practices of Leading Organizations*:

> Rather than conducting one large risk assessment covering all of an entity's operations at once, the organizations generally conducted a series of narrower assessments on various individual segments of the business. As a result, the scope of each assessment was limited to a particular business unit, system, or facility, or to a logically related set of operations [GAO 99[31]].

Conclusion

Risk-centered practices assume the presence of an appropriate risk assessment method, selected to satisfy business objectives and security, legal, and regulatory requirements. The selected risk assessment method should ensure that subsequent assessments "produce comparable and reproducible results" [ISO 05b[32]].

To be effective and sustainable, risk-centered practices must be deployed using a continuous, plan-do-check-act[33] approach through the useful life of the system.

Table 1: Risk-Centered Practices that Aid in Security Practice Selection for Deployment and Operations

Table 1 lists risk-centered practices and pointers to sources that provide detailed descriptions and implementation guidance. Practices are listed in the order recommended for implementation. Each source is fully cited on its first occurrence and summarized thereafter.

Table 1. Risk-centered practices that aid in security practice selection for deployment and operations

Practice	Sources
Define the scope of the risk assessment. Ensure a clear and direct tie to business and mission objectives.	• "Introduction to the OCTAVE® Approach" [Alberts 03[34]] • *Software Security:Building Security In*, Chapter 2, "A Risk Management Framework" [McGraw 06[35]] • ISO 13335-3 (9.3.1) *Guidelines for information security risk management* [BSI 98[36]] • FIPS 199 *Security Categorization of Federal*

[31] daisy:583#GAO99 (Deployment & Operations References)

[32] daisy:583#ISO05b (Deployment & Operations References)

[33] daisy:574 (Plan, Do, Check, Act)

[34] daisy:583#Alberts03 (Deployment & Operations References)

[35] daisy:583#McGraw06 (Deployment & Operations References)

[36] daisy:583#BSI98 (Deployment & Operations References)

Identify information assets that are important to the organization. Focus risk assessment on those assets judged to be the most critical: - asset value - business and legal requirements - impact of loss of confidentiality, integrity, availability	*Information and Information Systems* [NIST 03[37]] - *Software Security*, Chapter 2 [McGraw 06[38]] - BS 7799-3 *Guidelines for information security risk management* [BSI 06[39]] - ISO 13335-3 (9.3.2, 9.3.3, Annex B) [BSI 98[40]] - OCTAVE [Alberts 03[41]]
Identify asset owners and custodians.	- FIPS 199 [NIST 03[42]] - BS 7799-3 [BSI 06[43]] - ISO 27001 *Information security management systems* [ISO 05b[44]]
Determine the criteria for accepting risks and the acceptable levels of risk, often referred to as risk tolerances or risk thresholds.	- BS 7799-3 [BSI 06[45]] - ISO 13335-3 [BSI 98[46]] - ISO 27001 [ISO 05b[47]]
Identify the relationships among critical assets, the threats to those assets, and vulnerabilities (both organizational and technological) that can expose assets to threats.	- OCTAVE [Alberts 03[48]] - BS 7799-3 [BSI 06[49]] - *Software Security*, Chapter 2 [McGraw 06[50]] - ISO 13335-3 (9.3.4, 9.3.5, Annexes C, D) [BSI 98[51]] - ISO 27001 [ISO 05b[52]]
Assess the likelihood of threats [53] and vulnerabilities.	- OCTAVE [Alberts 03[54]] - BS 7799-3 [BSI 06[55]] - *Software Security*, Chapter 2 [McGraw 06[56]] - ISO 13335-3 [BSI 98[57]]
Identify the impacts due to losses resulting from realized risks.	- OCTAVE [Alberts 03[58]] - BS 7799-3 [BSI 06[59]] - *Software Security*, Chapter 2 [McGraw 06[60]] - ISO 13335-3 [BSI 98[61]] - ISO 27001 [ISO 05b[62]]
Identify risks and evaluate options for treatment of risks (accept, mitigate, avoid, transfer, share with a third party (such as a supplier)).	- BS 7799-3 [BSI 06[63]] - OCTAVE [Alberts 03[64]] - ISO 13335-3 (9.3.7, Annex E) [BSI 98[65]] - ISO 27001 [ISO 05b[66]]
Identify practice-based protection strategies (control objectives and controls) that reduce risks to critical assets to levels that are within acceptable tolerances. Controls can be deployed to	- OCTAVE [Alberts 03[67]] - BS 7799-3 [BSI 06[68]] - *Software Security*, Chapter 2 [McGraw 06[69]]

[37] daisy:583#NIST03 (Deployment & Operations References)

[38] daisy:583#McGraw06 (Deployment & Operations References)

[39] daisy:583#BSI06 (Deployment & Operations References)

[40] daisy:583#BSI98 (Deployment & Operations References)

[41] daisy:583#Alberts03 (Deployment & Operations References)

[42] daisy:583#NIST03 (Deployment & Operations References)

[43] daisy:583#BSI06 (Deployment & Operations References)

[44] daisy:583#ISO05b (Deployment & Operations References)

[45] daisy:583#BSI06 (Deployment & Operations References)

[46] daisy:583#BSI98 (Deployment & Operations References)

[47] daisy:583#ISO05b (Deployment & Operations References)

[48] daisy:583#Alberts03 (Deployment & Operations References)

[49] daisy:583#BSI06 (Deployment & Operations References)

[50] daisy:583#McGraw06 (Deployment & Operations References)

[51] daisy:583#BSI98 (Deployment & Operations References)

[52] daisy:583#ISO05b (Deployment & Operations References)

[53] Threats include characterizing an organization's "adversaries, their potential motivations, and their classes of attack." http://nsa2.www.conxion.com/support/guides/sd-1.pdf.

[54] daisy:583#Alberts03 (Deployment & Operations References)

[55] daisy:583#BSI06 (Deployment & Operations References)

[56] daisy:583#McGraw06 (Deployment & Operations References)

[57] daisy:583#BSI98 (Deployment & Operations References)

[58] daisy:583#Alberts03 (Deployment & Operations References)

[59] daisy:583#BSI06 (Deployment & Operations References)

[60] daisy:583#McGraw06 (Deployment & Operations References)

[61] daisy:583#BSI98 (Deployment & Operations References)

[62] daisy:583#ISO05b (Deployment & Operations References)

[63] daisy:583#BSI06 (Deployment & Operations References)

[64] daisy:583#Alberts03 (Deployment & Operations References)

[65] daisy:583#BSI98 (Deployment & Operations References)

[66] daisy:583#ISO05b (Deployment & Operations References)

[67] daisy:583#Alberts03 (Deployment & Operations References)

[68] daisy:BSI06#BSI06

[69] daisy:583#McGraw06 (Deployment & Operations References)

reduce likelihood and impact.	• ISO 27001 [ISO 05b[70]] • ISO 13335-4 *Selection of safeguards* [ISO 00[71]]
Identify potential tradeoffs between reducing risk, increased costs, and decreased operational effectiveness.	• NIST 800-27 (Principle 7) *Engineering Principles for Information Technology Security* [Stoneburner 04[72]]
Identify approaches for managing residual risks that remain after protection strategies are adopted.	• BS 7799-3 [BSI 06[73]]
Measure, review, and revise risk-centered practices. Take into account changes to the organization, business objectives and processes, regulatory and marketplace factors, threats, technology, and control effectiveness. Re-assess risks periodically.	• BS 7799-3 [BSI 06[74]] • *Software Security*, Chapter 2 [McGraw 06[75]] • ISO 27001 [ISO 05b[76]]

Carnegie Mellon Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

Fields

Name	Value
Copyright Holder	SEI

Fields

Name	Value
is-content-area-overview	false
Content Areas	Best Practices/Deployment & Operations
SDLC Relevance	Deployment
Workflow State	Publishable

[70] daisy:583#ISO05b (Deployment & Operations References)

[71] daisy:583#ISO00 (Deployment & Operations References)

[73] daisy:583#BSI06 (Deployment & Operations References)

[74] daisy:583#BSI06 (Deployment & Operations References)

[75] daisy:583#McGraw06 (Deployment & Operations References)

[76] daisy:583#ISO05b (Deployment & Operations References)

[1] http://www.sei.cmu.edu/about/legal-permissions.html

Sort Order	4